LESSON 38 – ELECTRONIC COUNTERMEASURES (ECM)/ELECTRONIC COUNTER-COUNTERMEASURES (ECCM)

To this point we've built a very solid basis for understanding radar. Now that we know how it works, we can look at ways to defeat it! We'll also look at the continual tug between offense and defense as we examine ways to avoid having your radar defeated.

Reading: Stimson **Ch. 34-35**
Problems/Questions: Work on Problem Set 5
Objectives:

38-1 Know the definition of ECM.
38-2 Know the three methods used to employ ECM.
38-3 Know the main types of jamming and how they affect a radar presentation.
38-4 Know the definition of ECCM.
38-5 Understand the methods used to counter noise and deception jamming.
38-6 Know the most effective ECCM of all.

Last Time: Electronic Support Measures
Interferometry
Reverse phased-array
The Mighty Wild Weasel

Today: ECM/ECCM
Chaff, noise, deception

Review of radar concepts

Physical Concept	*ECM Technique Exploiting Concept*
Diffraction	
finite beamwidth	angle deception, noise
sidelobes	angle deception, noise
Pulsed Operation	
range gates	range deception, noise
finite spectral width	range deception
Doppler Shift	
frequency filters	velocity deception
clutter	chaff
Phased Arrays	
Phase detection	phase deception
Dynamic Range	
Min/Max useable signal	range/velocity deception, noise

Now that we've seen how radars work in excruciating detail, we'll tak a look at how they can be defeated. Electronic Countermeasures, or ECM, can basically be broken down into four subsets: jamming (radiation or reradiation of signals by a countermeasures pod or dedicated jamming platform to fool the enemy radar); expendables (dispensing chaff, flares, or a towed decoy); avoidance/evasion (hiding from the enemy's EM threats while accomplishing your mission (i.e. flying under radar coverage, terrain masking, using "stealth"); and destruction (eliminating EM threats through firepower, a mission called Suppression of Enemy Air Defenses, or SEAD).

Chaff

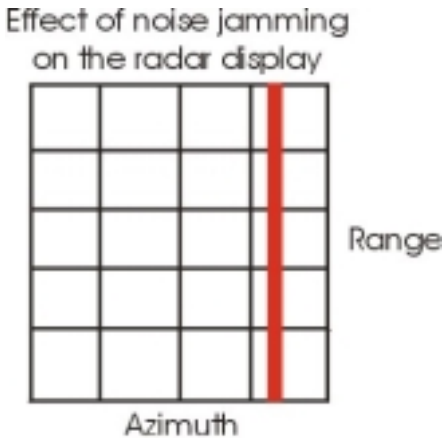
The simplest ECM is chaff. Chaff is made up of billions of metallic fibers that are ejected into the air around an aircraft. The length of the fibers control which frequencies are most heavily reflected. *Against non-Doppler radars*, chaff is extremely effective. It rapidly "blooms", or expands in space, creating a huge radar return that can mask actual aircraft returns. Individual chaff fibers, being of extremely low mass, rapidly decelerate, quickly attaining the velocity of the air mass into which they were ejected. Chaff clouds stay aloft and intact for long periods of time as well. It is not uncommon to see multiple sequential intercept practices get more and more complicated as the clouds from previous engagements complicate the initial radar picture.

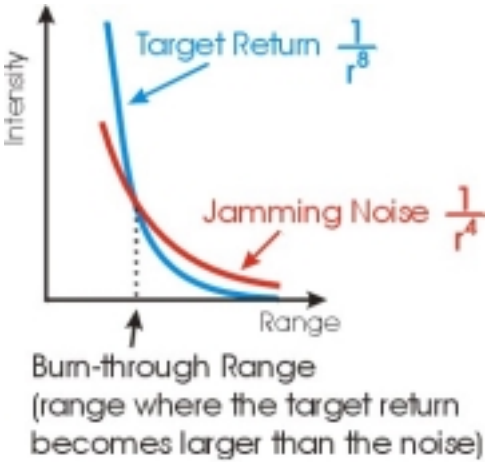
Chaff is less effective against Doppler radars due to its rapid deceleration. Initially, it moves with the same speed as the ejecting jet, and hence has the same Doppler shift. However, it quickly decelerates, moving toward the location of the main lobe clutter (MLC). In high wind conditions, it can move sufficiently quickly that it will be out of the target radar's notch and will show up on their screens, but this is not the norm. However, chaff is a very effective enhancement to the beam maneuver discussed earlier. It increases the amount of masking return near the location of MLC, making it that much easier to hide your return in the clutter.

There are two types of jamming: noise and deception. Noise just tries to drown-out the victim radar's signal, while deception tries to make the victim's radar display false information about you.

Noise

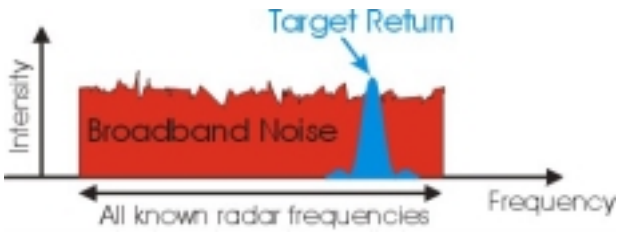
The simplest form of jamming is broadband noise. All that is done is to broadcast a loud, meaningless signal across a range of frequencies. The result is like trying to have a conversation on the flightline where a bunch of jets are taxiing: the useful signal is completely lost in the background. The trouble with noise is that someone has to broadcast it, which means that the bad guys know their position pretty accurately! They may not know the distance to you (think about how range is determined), but they know the angle to you very well. This sets the jammer up for getting popped by an ARM (anti-radiation missile), which homes in on the jamming signal.



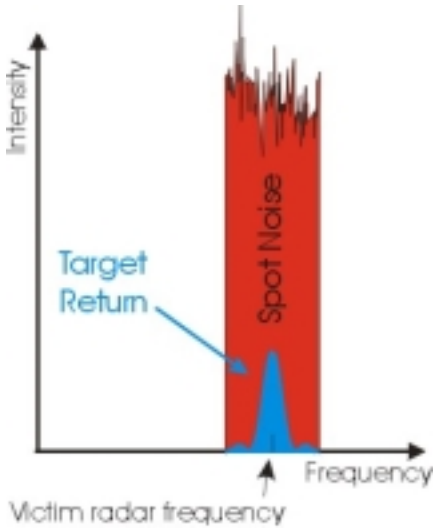


How much power is required for noise? Lots! You've got to get enough signal to the victim radar to overwhelm any return from the aircraft you're trying to protect. This process is aided by the fact that your jamming signal only has to travel one way to the victim(with an associated $1/r^4$ drop in power), while the victim radar's beam has to travel two ways to the aircraft it's trying to track, with a $1/r^4 \cdot 1/r^4 = 1/r^8$ power drop. However, the power you can emit is limited.

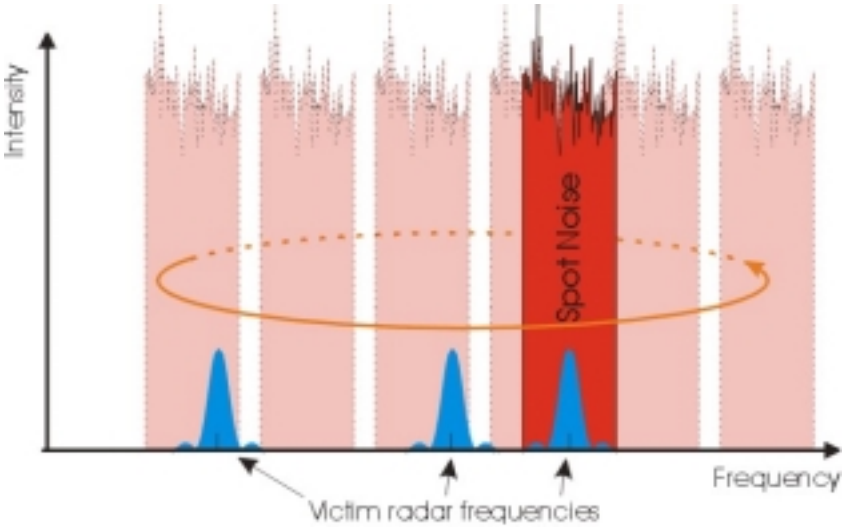
You've got two ways you can spend your power-generating capability: broadcast relatively low power over a lot of frequencies, or broadcast relatively high power over a few select frequencies. This figure shows the relatively low intensities generated by broadband noise jamming against a victim



If you know the frequency that the victim radar is using, you can be more selective about the frequency range you transmit, and, using the same total power, can get much higher intensities, which mean the screened aircraft can get much closer before their return starts to burn through the jamming.



If a radar uses more than one frequency, or if you need to target multiple radars with a limited power, you can use swept spot jamming. With this technique, the same high-intensity, low bandwidth noise spectrum is continually swept through the range of frequencies used by the victim radars. While it does not continually mask friendly presence from each radar, it can disrupt locks.



Should the victim radar have a slow automatic gain control (AGC), swept spot jamming can be very effective. Radars shield themselves against high-power inputs which could fry their receiver electronics by essentially turning down the volume. Imagine standing by your stereo playing the 1812 overture (the one with the cannons) very loudly. You know your speakers can't handle the boom of the cannons, so you're at the ready on the volume knob, ready to turn it down in time to protect the speakers. You're applying *manual* gain control. As another analogy, consider surfing the TV channels, you stop on FOX to watch the X-files. For some reason, FOX never sets the volume at the same level as everyone else. It's too loud. Consequently, you turn down your TV volume. After the show is over, you switch to another channel and realize you can't hear a thing! These are the same ideas as a jamming signal reducing the gain of the receiving antenna, but the radar does the same thing automatically. If its AGC has a slow relaxation (if it

takes a while before it's not too scared to turn up the volume [the gain] again), then swept spot jamming can be extremely effective, as many times the radar will not have turned up the gain before the spot sweeps over its frequency again.

If you have lots of power available, or if you're willing to spread it a bit thinner, and are trying to jam more than one frequency at a time, you can employ multiple spot jamming. This is a compromise between broadband jamming and spot jamming, giving more power on victim radar frequencies than the former but less than the latter.

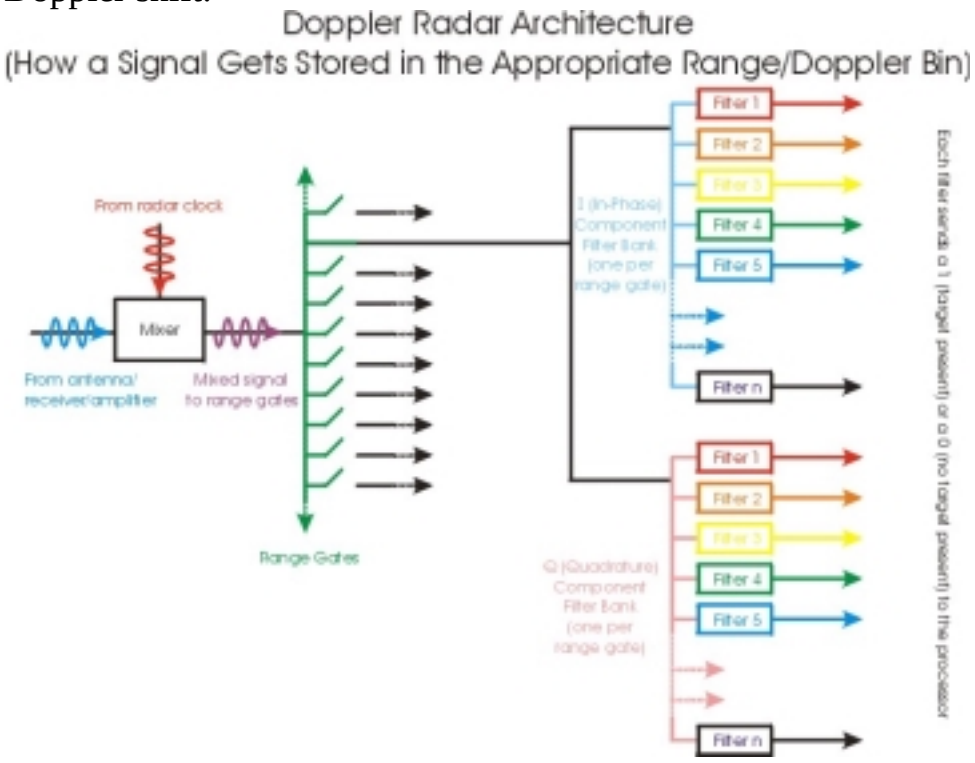
Even this sort of spot jamming is not very efficient, as the noise is transmitted for much longer than the victim radar is actually looking at you. To be even more efficient, you can use what is called *bin-masking*. Bin-masking has the jamming noise only transmit during times near when the victim radars pulses arrive. By knowing the PRF of the victim radar, the jamming pod can calculate when a pulse is about to arrive, and then turn on the noise so that it lasts until some time after the pulse has passed. Instead of the normal barrage noise strobe you saw earlier that extended over all ranges, you get a bar of noise that surrounds the actual target return.

Deception jamming is more difficult to implement, but far more effective against more modern radars. We'll only discuss a couple of deception modes in this lesson.

The simplest form of deception jamming is called a false-target repeater. When an incoming pulse from the victim radar is detected, the jamming pod memorizes the pulse characteristics and then retransmits a similar pulse at different times. These pulses return to the victim radar, which interprets

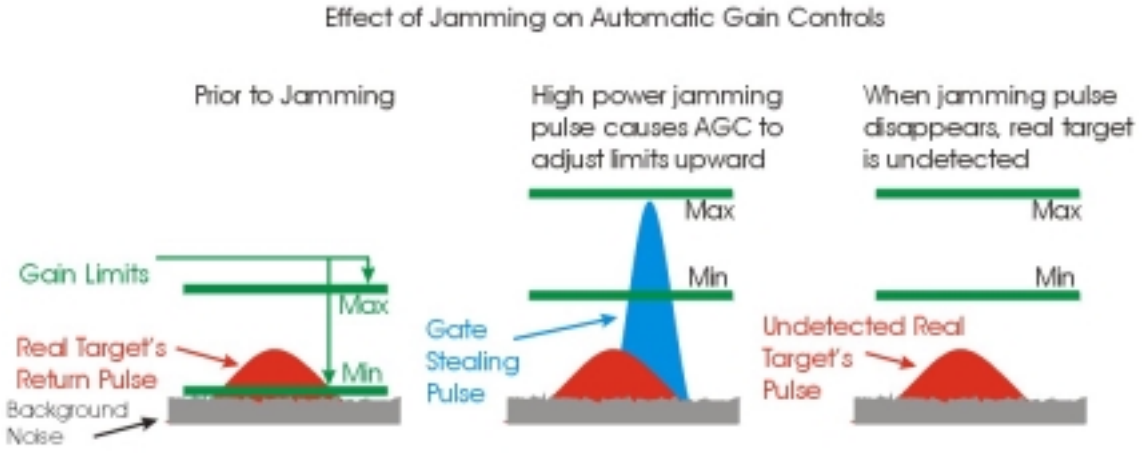
them as targets with the same angular position but different range as the real target.

A more complicated form of deception jamming is that of *gate stealing*. Recall that digital radars store target locations in on of many range-Doppler bins. There are a number of range gates that open and close sequentially to allow through signals with a specific time delay from the transmitted signal. Each of these range gates has a pair of associated frequency filter banks to resolve the Doppler shift of the received signal. The target location is then stored in the memory location corresponding to the target's range and Doppler shift.



Gate stealers rely on the same automatic gain control discussed earlier. The jamming pod detects an incoming pulse and quickly transmits a stronger pulse that otherwise looks like the received pulse. One effect of this initial pulse is to make your jet easier to see for the victim radar. The other effect is to get the victim radar's AGC to "turn down its volume". The intent of this AGC effect is to get your real return to be too weak for the victim's radar to consider it as anything but noise.

If you add jamming with a fast set-on, the signal stays the same, but the noise increases greatly, canceling the signal, or at least putting its amplitude under the false alarm threshold.

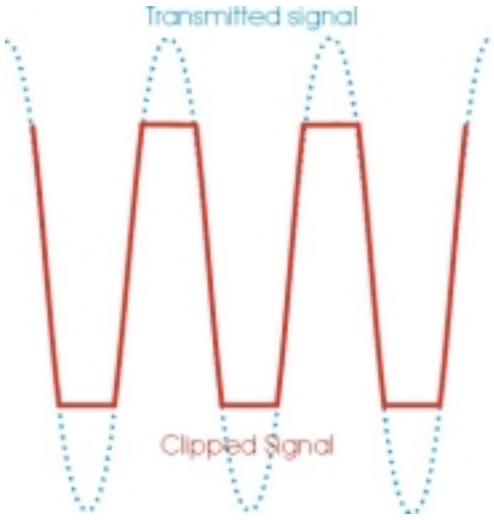


We've discussed one reason for AGC: to protect electronics from high-power signals that could fry them. There's another reason, too. Have you ever heard what happens to a speaker when you put too much power into it (not enough to blow it, mind you)? You get a clipping sound. It's called *clipping* because the speaker can't deliver the full amplitude of the wave, and the tops and bottoms of the sine waves get clipped off.

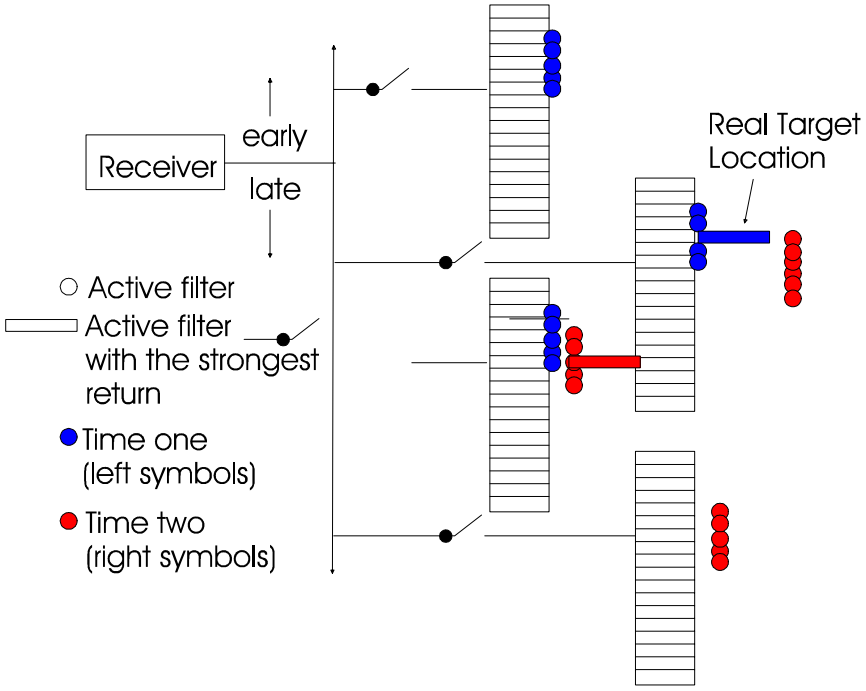
Clipping causes severe Doppler ambiguities, due to the extra frequencies required to generate the non-sinusoidal clipped wave.

Show clip.avi

In order to prevent clipping (and the associated Doppler ambiguities), the radar tries to keep its maximum allowable signal above the level of any returned signals. If your signal is just discernible at a certain gain, then a high-amplitude noise signal may push the gain down so that your victim is no longer detectable, as shown in the above figure. Once the gate stealer has done its job, it stops transmitting, and in the resulting delay before the AGC readjusts downward, the victim's radar breaks its lock on you.

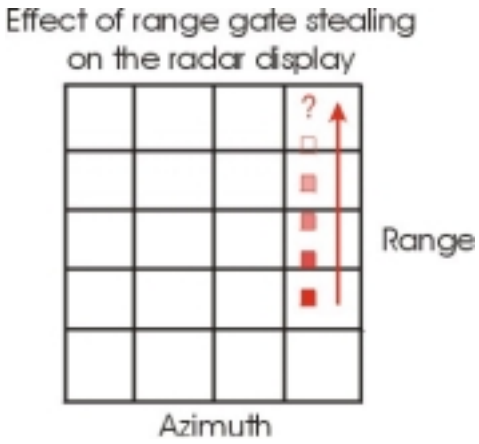


A variant of the basic gate stealers actually pull the range gate away from your real location and show you at a different range. This is done by capturing the gate with the AGC-defeating pulse as described above, and then slowly varying the timing of the jamming pulse until the range of the jamming pulse is quite different from your actual range. This increases the difficulty of a re-lock by the victim's radar because it doesn't actually look for targets in every point of space to save calculation time. It only looks where targets were known to be, or where they could have gone since it last looked for that particular target.



To be more specific, once a target is detected and is being tracked, the radar doesn't look at every range/Doppler bin again. It knows max accelerations possible for an aircraft, and only looks in those bins where the target could possibly be. We'll call these active filters because they're the only ones the computer actively forms and checks.

Range gate stealers begin by putting out a repeater signal at the true range, increase the repeater strength to drive down the gain, and then delay the strong signal, slightly increasing the delay for a time. Eventually they cut the delayed signal, causing the victim radar to lose the track.



ECCM

For every ECM technique, there exists a corresponding ECCM technique. If they don't exist now, they certainly will soon. It's a classic game of offense/defense, with the offense having the upper hand at times and then the defense figuring out how to get around the offense. Some basic ECCM techniques are listed below:

Noise can be combated by frequency agility – carrier changes frequency semi-randomly after each integration period. This makes it more difficult for noise jammers to identify and jam the signal. The relatively long integration times required to get the large number of pulses back from a target to sufficiently narrow the Doppler spectrum makes the jammer's job a bit easier, however, as it gives it time to find the new frequency.

One counter to gate stealers is called a leading edge detector. All jammers have a finite set-on time. That is, it takes a small delay for the jammer to recognize a pulse has arrived and to generate the amplified gate-stealing pulse. The counter uses what is called a leading edge tracker, which essentially differentiates the received signal. The slope of the received signal should have one positive region and one negative region, corresponding to the time where the pulse intensity rises and then falls. Due to the finite set-on time, a gate stealing pulse will have two positive regions. When the ECCM program in the victim radar senses the second onset pulse, it knows it's being jammed and shortens its range gate accordingly, ignoring the higher intensity deception pulse and only allowing the first part of the true target return to pass.

An even simpler counter to gate stealers and other techniques that target the AGC of the radar is to design your radar with a very large dynamic range, the distance between the maximum and minimum volumes the receiver can handle.

There are MANY other techniques for ECM and ECCM. The ones discussed above are merely presented as an introduction to the ongoing battle between offense and defense.